

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF NEW YORK

SUSAN B. LONG and )  
TRAC REPORTS, INC., )  
                        )  
Plaintiffs,           )  
                        )  
v.                     )  
                        )  
U.S. IMMIGRATION AND CUSTOMS )                         No. 5:23-cv-1564 (DNH/TWD)  
ENFORCEMENT and      )  
U.S. CUSTOMS AND BORDER   )  
PROTECTION,            )  
                        )  
Defendants.           )  
                        )

---

**PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO  
DEFENDANT U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT'S  
MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF  
PLAINTIFFS' CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT**

Nicolas A. Sansone  
(admitted pro hac vice)  
Michael T. Kirkpatrick  
(admitted pro hac vice)  
Public Citizen Litigation Group  
1600 20th Street NW  
Washington, DC 20009

*Counsel for Plaintiffs*

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	ii
PRELIMINARY STATEMENT .....	1
FACTUAL BACKGROUND.....	2
LEGAL STANDARDS .....	5
ARGUMENT.....	6
I.     ICE is not entitled to summary judgment. ....	6
A. ICE has not shown that producing records in response to Plaintiffs' FOIA request would be unduly burdensome. ....	6
1. ICE's claims of burdensomeness rest on a mischaracterization of what Plaintiffs ask ICE to produce.....	7
2. ICE's evidence on burden contains multiple incorrect assumptions about the EID. ....	8
3. ICE's burden arguments do not justify its failure to produce <i>any</i> responsive records.....	13
B. ICE has not shown that FOIA exemptions relieve it of its obligation to produce any responsive records.....	15
1. ICE has not shown that personal privacy and safety concerns justify withholding all requested records under Exemptions 7(C), 6, and 7(F). ....	16
2. ICE has not shown that law-enforcement concerns justify withholding all requested records under Exemptions 7(E) and 7(A).....	24
3. ICE has not shown that its grab-bag of miscellaneous statutory provisions justifies withholding all requested records under Exemption 3. ....	33
II.   Plaintiffs are entitled to partial summary judgment.....	35
III.   In the alternative, a ruling on summary judgment should be deferred pending discovery. ....	36
CONCLUSION.....	38

## TABLE OF AUTHORITIES

Cases	Page(s)
<i>Akel v. U.S. Department of Justice</i> , No. 20-cv-03240, 2024 WL 939974 (D.D.C. Mar. 4, 2024) .....	38
<i>American Civil Liberties Union Immigrants' Rights Project v. U.S. Immigration &amp; Customs Enforcement</i> , 58 F.4th 643 (2d Cir. 2023) .....	passim
<i>Associated Press v. U.S. Department of Defense</i> , 554 F.3d 274 (2d Cir. 2009).....	22, 23
<i>Associated Press v. U.S. Department of Justice</i> , 549 F.3d 62 (2d Cir. 2008).....	16
<i>Bloomberg L.P. v. U.S. Postal Service</i> , 118 F.4th 307 (2d Cir. 2024) .....	33
<i>Carney v. U.S. Department of Justice</i> , 19 F.3d 807 (2d Cir. 1994).....	6, 37
<i>Citizens for Responsibility &amp; Ethics in Washington v. U.S. Department of Justice</i> , 746 F.3d 1082 (D.C. Cir. 2014).....	31, 32
<i>Cook v. National Archives &amp; Records Administration</i> , 758 F.3d 168 (2d Cir. 2014).....	23
<i>Elliott v. Cartagena</i> , 84 F.4th 481 (2d Cir. 2023) .....	6, 37
<i>Families for Freedom v. U.S. Customs &amp; Border Protection</i> , 837 F. Supp. 2d 331 (S.D.N.Y. 2011).....	38
<i>Federal Bureau of Investigation v. Abramson</i> , 456 U.S. 615 (1982).....	18
<i>Federal Labor Relations Authority v. U.S. Department of Veterans Affairs</i> , 958 F.2d 503 (2d Cir. 1992).....	23
<i>Grand Central Partnership, Inc. v. Cuomo</i> , 166 F.3d 473 (2d Cir. 1999).....	32
<i>Hopkins v. U.S. Department of Housing &amp; Urban Development</i> , 929 F.2d 81 (2d Cir. 1991).....	19
<i>Lazaridis v. U.S. Department of State</i> , 934 F. Supp. 2d 21 (D.D.C. 2013).....	30

<i>Long v. U.S. Department of Justice,</i> 450 F. Supp. 2d 42 (D.D.C. 2006).....	23
<i>Long v. U.S. Immigration &amp; Customs Enforcement,</i> 464 F. Supp. 3d 409 (D.D.C. 2020).....	26, 30
<i>Maydak v. U.S. Department of Justice,</i> 218 F.3d 760 (D.C. Cir. 2000).....	30, 31, 33
<i>Mead Data Central, Inc. v. U.S. Department of the Air Force,</i> 566 F.2d 242 (D.C. Cir. 1977).....	19
<i>New York Legal Assistance Group v. Board of Immigration Appeals,</i> 987 F.3d 207 (2d Cir. 2021).....	14
<i>Osen LLC v. U.S. Central Command,</i> 969 F.3d 102 (2d Cir. 2020).....	5, 15
<i>Petrucelli v. U.S. Department of Justice,</i> 51 F. Supp. 3d 142 (D.D.C. 2014).....	23
<i>Project South v. U.S. Immigration &amp; Customs Enforcement,</i> No. 1:21-cv-08440, 2024 WL 1116164 (S.D.N.Y. Mar. 12, 2024).....	34
<i>Public Citizen Health Research Group v. U.S. Food &amp; Drug Administration,</i> 185 F.3d 898 (D.C. Cir. 1999).....	5
<i>SafeCard Services, Inc. v. U.S. Securities &amp; Exchange Commission,</i> 926 F.2d 1197 (D.C. Cir. 1991).....	17
<i>Seife v. U.S. Food &amp; Drug Administration,</i> 43 F.4th 231 (2d Cir. 2022) .....	5, 15, 35
<i>Sussman v. U.S. Marshals Service,</i> 494 F.3d 1106 (D.C. Cir. 2007).....	31
<i>Weisberg v. U.S. Department of Justice,</i> 745 F.2d 1476 (D.C. Cir. 1984).....	17, 18

## Statutes

5 U.S.C. § 552(a)(8)(A)(i)(I) .....	15, 23, 30
5 U.S.C. § 552(a)(8)(A)(ii)(I) .....	13
5 U.S.C. § 552(a)(8)(B) .....	15
5 U.S.C. § 552(b) .....	15

5 U.S.C. § 552(b)(3)(A).....	33
5 U.S.C. § 552(b)(6) .....	16
5 U.S.C. § 552(b)(7)(A).....	24
5 U.S.C. § 552(b)(7)(C) .....	16
5 U.S.C. § 552(b)(7)(E) .....	24, 25
5 U.S.C. § 552(b)(7)(F).....	16

## **Regulations**

6 C.F.R. § 5.4(i)(2)(ii).....	10, 14
-------------------------------	--------

## **Rules**

Federal Rule of Civil Procedure 26(b)(1) .....	37
Federal Rule of Civil Procedure 56(a).....	5
Federal Rule of Civil Procedure 56(d).....	6

## **Other Authorities**

U.S. Customs & Border Protection, <i>CBP Office of Field Operations Statistics</i> (last updated Nov. 4, 2024) .....	31
U.S. Customs & Border Protection, <i>Nationwide Encounters</i> (last updated Oct. 22, 2024) .....	11
U.S. Customs & Border Protection, <i>Nationwide Encounters Data Dictionary</i> (Sept. 2023).....	11
U.S. Department of Homeland Security, <i>Privacy Impact Assessment for the CBP Portal (e3) to EID/IDENT</i> (Aug. 2, 2021).....	11
U.S. Department of Homeland Security, <i>Privacy Impact Assessment for the Enforcement Integrated Database</i> (Jan. 14, 2010)... 3, 9, 27	
U.S. Department of Justice, <i>FY 2022 Annual Performance Report</i> (2023).....	13
U.S. Immigration & Customs Enforcement, <i>ERO Removes Noncitizen Wanted for Homicide to El Salvador</i> (Oct. 18, 2024) .....	21

U.S. Immigration & Customs Enforcement, <i>ERO Boston Arrests Brazilian National Charged with Drug, Firearms, Ammunition Crimes in Martha's Vineyard</i> (Oct. 4, 2024) .....	21
U.S. Immigration & Customs Enforcement, <i>Organizational Structure</i> (last updated Aug. 20, 2024) .....	28
U.S. Immigration & Customs Enforcement, Request to National Archives & Records Administration for Records Disposition Authority (Feb. 23, 2010).....	9

## PRELIMINARY STATEMENT

Over a year ago, Plaintiffs Susan B. Long and TRAC Reports, Inc., submitted a request to Defendant U.S. Immigration and Customs Enforcement (ICE) pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552, seeking records from the Enforcement Integrated Database (EID), a government database containing immigration enforcement records.<sup>1</sup> ICE did not respond, and Plaintiffs filed this lawsuit to seek production of the requested records. ICE has now moved for summary judgment, arguing that it need not produce *any* of the requested records because it would be unduly burdensome to produce *all* of the requested records and because *some* of the requested records are exempt from disclosure. This Court should deny ICE's motion.

ICE's contention that it would consume too much time and computing power to produce the requested records is based on a declaration that describes the difficulties involved in pulling all the requested records together into a single massive document that would be released at one time. The declaration does not speak to the feasibility of what Plaintiffs requested: a phased rollout of individual EID tables. Even on its own terms, moreover, the declaration contains numerous faulty assumptions about the EID and its functionality, and the declaration does not even purport to consider the feasibility of producing a segregable subset of the requested records.

ICE also attempts to justify its refusal to produce any responsive records by invoking FOIA exemptions that permit an agency to withhold records that could compromise personal privacy or safety, adversely affect law-enforcement interests, or reveal information that other statutes shield from disclosure. These arguments, too, lack merit. ICE regularly produces vast quantities of EID data without compromising the interests that it now invokes to justify its failure

---

<sup>1</sup> David Burnham, who was originally a plaintiff in this lawsuit, passed away on October 1, 2024. See Dkt. 41. His claims will be dismissed on January 6, 2025, barring substitution of a proper party in his place. See Dkt. 42.

to produce any EID records. And even if FOIA permits certain redactions, ICE has not carried its burden of demonstrating that *no* responsive records can be produced without causing reasonably foreseeable harm to the interests served by FOIA’s exemptions.

Meanwhile, Plaintiffs are entitled to partial summary judgment. Even taking ICE’s evidence at face value and setting aside the numerous factual disputes that call its accuracy into question, the evidence cannot justify ICE’s wholesale refusal to produce any records. Evidence that it would be burdensome to produce everything that Plaintiffs have requested does not create a fact dispute over whether ICE can produce discrete, segregable portions of the EID records that Plaintiffs seek. And evidence that certain fields of information are exempt from disclosure does not create a factual dispute over whether ICE can produce the undisputedly nonexempt fields. Plaintiffs are thus entitled to the immediate production of the nonexempt portions of any responsive records that ICE undisputedly *can* release without undue burden.

If the Court nonetheless finds that disputes of material fact foreclose a grant of partial summary judgment to Plaintiffs on the current record, it should defer ruling on the parties’ cross-motions until discovery is complete. This Court authorized Plaintiffs to serve discovery demands on ICE, and Plaintiffs have done so. ICE has not yet responded. The requested discovery will cast meaningful light on factual contentions ICE has made in support of its arguments, and Plaintiffs should have the opportunity to respond to those arguments on a complete record.

## **FACTUAL BACKGROUND**

The EID is a database that “captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations” conducted by ICE, U.S. Customs and Border Protection (CBP), and other components of the U.S. Department of Homeland

Security (DHS). DHS, *Privacy Impact Assessment for the Enforcement Integrated Database* at 2 (Jan. 14, 2010) (hereafter, *EID Privacy Impact Assessment*), <https://tinyurl.com/57d3z7vk>. It is organized into a series of discrete database tables, each of which is organized as a series of rows and columns. Long Decl. ¶ 10. Each row is a “record” that contains a collection of information about a specific person or event, depending on the topic around which the table is organized. *Id.* Each column corresponds to a particular “field” of information contained in the records. *Id.*

On September 21, 2023, Plaintiffs submitted a FOIA request to ICE, seeking “a copy of each table and field of information stored in the current [EID].” Dkt. 40-5 at 1. Plaintiffs “ask[ed] that the data be output table by table” so that the records produced would “retain[] the structure of the underlying data.” *Id.* at 2. ICE acknowledged receiving the request but did not otherwise reply. Sansone Decl. ¶¶ 3–4 & Exh. A.

Plaintiffs then filed this lawsuit, claiming that ICE had violated FOIA by failing to produce the requested records. Dkt. 1 ¶¶ 16–17. After ICE filed its answer, Dkt. 18, the parties agreed to meet and confer regarding settlement, Sansone Decl. ¶ 6. On April 19, 2024, Plaintiffs made a written settlement proposal that reduced the volume of the requested records, invited feedback about ways that the proposal could be better tailored to suit ICE’s needs, and expressed Plaintiffs’ openness to further refining the proposal in light of such feedback. *Id.* ¶ 7. About two months later, ICE indicated at a June 17, 2024, status conference that it could not provide an estimate of when it would be able to respond to this settlement proposal. *Id.* ¶ 9. Plaintiffs then proposed three alternative possibilities for limited production that ICE could make in the interim to facilitate the settlement process. *Id.* ¶ 10. ICE rejected all three proposals on July 22, 2024, without offering counterproposals, and the parties concluded during a July 26, 2024, meet-and-confer that they had reached an impasse and should proceed to dispositive motions. *Id.* ¶ 11.

During that same meet-and-confer, Plaintiffs stated that in order to narrow the issues before the Court, they would focus their legal challenge solely on ICE’s failure to produce a discrete subset of the records that Plaintiffs had originally requested. *Id.* ¶¶ 11–12. By letter dated August 1, 2024, Plaintiffs agreed to challenge only ICE’s failure to produce:

- (1) All datapoints (from any time) that are directly or indirectly linked to a person for whom [ICE] ha[s] established an official case seeking that person’s removal from the country.
- (2) All datapoints (from any time) that are directly or indirectly linked to a person who was apprehended pursuant to a CBP “encounter” in or after Fiscal Year 2020, with “encounter” used to mean the same thing that CBP uses it to mean in its Nationwide Encounters Dataset.
- (3) All code files, lookup tables, or other records that translate the specific codes used in connection with the datapoints contained in paragraphs (1) and (2) above into their corresponding meaning.

Dkt. 40-7 at 2. The letter further indicated that Plaintiffs would not challenge ICE’s decision to redact “free-format fields or, in other words, fields that contain potentially unique individualized content entered into each cell, as distinct from standardized-content fields that allow only standardized entries (such as dates, times, numbers, codes, or categories).” *Id.* ICE accepts that the August 1 letter is the operative FOIA request for all present purposes. Dkt. 40-1 at 3 n.2.

On October 1, 2024, ICE moved for summary judgment. Dkt. 40. Along with the motion, ICE filed three declarations from agency personnel, each of which made numerous factual representations in support of ICE’s motion. *See* Dkts. 40-2 (Fontaine Decl.), 40-3 (Gibney Decl.), 40-8 (Lynch Decl.). Following a meet-and-confer, Plaintiffs filed an October 9, 2024, motion, asking that summary judgment briefing be deferred to permit Plaintiffs an opportunity to probe the factual representations in ICE’s declarations. Dkt. 43. Magistrate Judge Dancks denied the motion but authorized Plaintiffs to serve discovery demands. Dkt. 45. Plaintiffs served

discovery demands on ICE on October 31, 2024, and ICE has yet to respond. Sansone Decl. ¶¶ 22–26 & Exhs. H, I, J. ICE’s deadline to do so is December 2, 2024. Sansone Decl. ¶ 26.

## LEGAL STANDARDS

FOIA “generally provides that ‘each agency, upon any request for records … shall make the records promptly available to any person.’” *Osen LLC v. U.S. Central Command*, 969 F.3d 102, 107 (2d Cir. 2020) (omission in original; quoting 5 U.S.C. § 552(a)(3)(A)). This statutory mandate “calls for broad disclosure of Government records.” *Id.* (quoting *CIA v. Sims*, 471 U.S. 159, 166 (1985)). Accordingly, under FOIA, the government “has the burden of ‘justify[ing] the withholding of any requested documents,’” *Seife v. FDA*, 43 F.4th 231, 235 (2d Cir. 2022) (alteration in original; quoting *U.S. Dep’t of State v. Ray*, 502 U.S. 164, 173 (1991)), with “[a]ll doubts … resolved in favor of disclosure,” *id.* (quoting *Bloomberg, L.P. v. Bd. of Governors of the Fed. Reserve Sys.*, 601 F.3d 143, 147 (2d Cir. 2010)).

As in any case, summary judgment in a FOIA case is proper only if “the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). Where the government is the movant, it accordingly must show that the undisputed facts establish a justification for failing to produce each record sought. *See Pub. Citizen Health Rsch. Grp. v. FDA*, 185 F.3d 898, 904 (D.C. Cir. 1999). But where the requester is the movant, “[t]he burden upon the requester is merely ‘to establish the absence of material factual issues before a summary disposition of the case could permissibly occur.’” *Id.* at 904–05 (quoting *Nat’l Ass’n of Gov’t Emp’ees v. Campbell*, 593 F.2d 1023, 1027 (D.C. Cir. 1978)).

Although agency declarations that “describe the justifications for nondisclosure with reasonably specific detail” can be a basis for awarding summary judgment in the government’s

favor, *ACLU Immigrants' Rights Project v. ICE*, 58 F.4th 643, 651 (2d Cir. 2023) (quoting *Knight First Amendment Inst. v. USCIS*, 30 F.4th 318, 327 (2d Cir. 2022)), summary judgment for the government is improper where the requester “make[s] a showing of bad faith on the part of the agency sufficient to impugn the agency’s affidavits or declarations or provide[s] some tangible evidence that an exemption claimed by the agency should not apply or summary judgment is otherwise inappropriate,” *Carney v. DOJ*, 19 F.3d 807, 812 (2d Cir. 1994) (citations omitted). In addition to denying the government’s motion for summary judgment in such cases, a court has discretion to order discovery into the government’s claimed defenses. *Id.* at 812–13.

Finally, under Federal Rule of Civil Procedure 56(d), a court may defer ruling on a summary judgment motion to permit time for discovery “[i]f a nonmovant shows by affidavit or declaration that … it cannot present facts essential to justify its opposition.” Fed. R. Civ. P. 56(d). Critically, “[w]hen a party has not had *any* opportunity for discovery, summary judgment is generally premature.” *Elliott v. Cartagena*, 84 F.4th 481, 493 (2d Cir. 2023).

## ARGUMENT

### I. ICE is not entitled to summary judgment.

ICE does not dispute that it has produced *no* responsive records in the year-plus since Plaintiffs filed their initial FOIA request. Instead, ICE argues that honoring Plaintiffs’ operative FOIA request would be unduly burdensome, Dkt. 40-1 at 9–15, and that some of the requested records are exempt from disclosure under various FOIA provisions, *id.* at 15–38. Both arguments rest on disputed facts, and neither establishes that ICE is entitled to judgment as a matter of law.

#### A. ICE has not shown that producing records in response to Plaintiffs’ FOIA request would be unduly burdensome.

ICE’s argument that producing records in response to Plaintiffs’ FOIA request would be unduly burdensome relies entirely on the declaration of Timothy Gibney, which states that

producing the requested records would require an estimated 8,360 hours of work. *See* Gibney Decl. ¶ 50. This estimate, however, is based on a misunderstanding of what Plaintiffs seek. Moreover, even on its own terms, Mr. Gibney’s estimate is wildly inflated in numerous respects. And in addition to being both misdirected and inaccurate, Mr. Gibney estimates the amount of time to produce *all* responsive records; he does not address whether ICE’s existing capabilities would permit ICE to produce *some* of the records with minimal expenditure of time and effort.

**1. ICE’s claims of burdensomeness rest on a mischaracterization of what Plaintiffs ask ICE to produce.**

Plaintiffs’ initial FOIA request asked that EID data “be output table by table” in a way that “retains the structure of the underlying data.”<sup>2</sup> Dkt. 40-5 at 2. Mr. Gibney, though, discusses the amount of time he imagines it would take to aggregate data from the EID’s multiple dispersed tables into a *single* table in which each case or encounter would correspond to a single row “contain[ing] denormalized data from tables found to have a direct or indirect relationship” with that case or encounter. Gibney Decl. ¶ 43; *see id.* ¶ 25 (describing queries that produce data “in a single table for consumption”). To present the data in this sort of “tabular format,” *id.* ¶ 34 n.5, Mr. Gibney claims that he would need to build queries “to join data together from different tables in the database,” *id.* ¶ 34. And according to Mr. Gibney, the process of analyzing the EID for these purposes and building and testing the queries that would create the sort of master table that he envisions would take about 8,360 hours of work. *Id.* ¶ 50.

Nowhere, though, does Mr. Gibney’s declaration address how much time it would take to produce what Plaintiffs actually seek: data that is reproduced from the EID without modification to its existing organizational structure. For example, the EID contains a table called the “CSE”

---

<sup>2</sup> Plaintiffs did not repeat this language in the operative FOIA request that superseded the initial request, *see* Dkt. 40-7, but nothing in the operative FOIA request suggests that Plaintiffs seek the production of the EID data in any other format.

table, in which each row relates to a single removal case. Long Decl. ¶ 16 & Exh. K. Part (1) of the operative FOIA request, which seeks records that are linked directly or indirectly to removal cases, essentially requests copies of the “CSE” table and those tables that are directly or indirectly linked to the “CSE” table. Mr. Gibney’s declaration is silent on the question of what would be involved in simply copying EID tables and transmitting them a few at a time to a FOIA requester. Indeed, ICE personnel have testified that extracting data “from a transactional system such as EID” and loading it into a “reporting system” is a “standard process” that ICE undertakes without incident “three times a week,” even where that process involves “transform[ing]” the data in ways that are not required here. Sansone Decl. Exh. B at 32–33.

Were ICE to copy the relevant tables and produce them on a rolling basis, ICE would not need to engage in the supposedly laborious query-building process that Mr. Gibney describes. As Mr. Gibney himself emphasizes, the EID is a transactional database that is “not optimized for analytics and reporting,” and “attempting complex queries or large-scale data aggregation” within such a database “can be challenging and may not deliver the performance needed for effective analysis.” Gibney Decl. ¶ 19. These limitations on the EID’s ability to synthesize data are among the reasons why Plaintiffs do not seek—and have never sought—a single massive, aggregated report of the sort that Mr. Gibney describes. Mr. Gibney’s estimate of the amount of time it would take to produce such a report is therefore entirely beside the point.

## **2. ICE’s evidence on burden contains multiple incorrect assumptions about the EID.**

Further undermining the value of Mr. Gibney’s declaration, it makes several assumptions about the EID that are flatly contradicted by representations that ICE has made elsewhere.

From the outset, Mr. Gibney incorrectly represents the EID’s size. He claims that the EID contains “over 1,000 data tables,” Gibney Decl. ¶ 13, and because he assumes that 75 percent of

the data tables contain records that are responsive to Plaintiffs' operative FOIA request, he speculates that "750 tables would need to be analyzed" to produce the requested records, *id.* ¶ 46. But according to productions ICE has made to Plaintiffs in ongoing litigation in the U.S. District Court for the District of Columbia, the EID contains a maximum of 399 data tables—barely more than a third of the number that Mr. Gibney supposes. *See* Long Decl. ¶ 14.<sup>3</sup>

Moreover Mr. Gibney appears to assume, incorrectly, that the EID is "not structured" to output data that is linked to a particular individual. Gibney Decl. ¶ 7; *see id.* ¶ 11 (claiming that the EID's data is "not kept or maintained in a way that would allow ICE to simply search for the [requested] data using existing capabilities"). But ICE has repeatedly acknowledged that the EID is readily capable of isolating data that pertains to a given person. For example, ICE has stated that, although the EID generally contains "event-based record[s]," the system "provides users the capability to access a person-centric view of the data as well." *EID Privacy Impact Assessment* at 2; *accord* ICE, Request to Nat'l Archives & Records Admin. for Records Disposition Auth., att. 1 at 1 (Feb. 23, 2010), <https://tinyurl.com/463e3k9v>. Declarations from ICE witnesses in prior FOIA litigation have attested to this point. *See* Sansone Decl. Exh. E at 4 & Exh. F ¶ 7.

Indeed, ICE has explained that the computer applications that it regularly utilizes enable a user to "view the entire detention history of a subject in ICE custody (all prior or current detention record data captured in the EID)" or to upload information to "[a] subject's EID record."<sup>4</sup> *EID Privacy Impact Assessment* at 4; *see also* Sansone Decl. Exh. C at 24 (ICE

<sup>3</sup> The EID also contains at least 450 "code" tables. Long Decl. ¶ 14. Unlike data tables, code tables do not contain records that relate to particular individuals, cases, or events. They simply translate coded values used in the data tables into plain English. *See id.* ¶ 13 & Exh. L. As part of the District of Columbia litigation concerning Plaintiffs' 2010 FOIA requests, ICE has provided Plaintiffs with partially redacted copies of many of the EID's code tables. *See* Long Decl. ¶ 13.

<sup>4</sup> ICE uses the term "subject" to refer to "an alleged immigration violator." *EID Privacy Impact Assessment* at 2.

witness's testimony regarding an application that permits a user to "enter[] an identifier such as an alien number or an FBI number, or a subject ID," and "retrieve data from the EID that allows them to see ... information related to ... the encounters that are linked to that person"). Even if the EID is not presently equipped to enable a user to pull up *all* datapoints directly or indirectly linked to a particular person, Mr. Gibney does not address whether ICE could draw on its existing queries to create such a capability without a great deal of additional coding. *See* 6 C.F.R. § 5.4(i)(2)(ii) ("Creating a computer program that produces specific requested fields or records contained within a well-defined database structure usually is considered business as usual.").

In fact, Plaintiffs deliberately tailored their operative FOIA request so that the data they sought would be easy to locate within the EID. The first set of records that Plaintiffs seek are those datapoints that are directly or indirectly linked to "a person for whom [ICE] ha[s] established an official case seeking that person's removal from the country." Dkt. 40-7 at 2. Removal cases are all listed within a single EID data table—the "CSE" table—where each case is given a "unique identifier" in the form of a system-generated number (the "CSE\_ID") and where each case is associated with a particular noncitizen who is also identified by a system-generated number (the "CSE\_IMMIGRATION\_CIV\_ID"). Long Decl. Exh. M at 3. Moreover, the "CSE" table associates every case—and thus every individual to whom Part (1) of Plaintiffs' operative FOIA request relates—with "user friendly reference number[s]" that can be used to access associated "case action" data and "custody action" data. *Id.* at 2–3. As an ICE witness in a prior FOIA litigation in this District explained this system, the EID permits a user to "run[] ... an alien number" and "bring up everything that's related to that [alien] number, or everything ever populated with it," and then "create a case" that connects the encounters associated with that alien number. Sansone Decl. Exh. C at 55. That case's numerical unique identifier, in turn,

“copies back to the EID” and provides a mechanism for “linking” other related records. *Id.* at 56. Because the unique case identifiers that are all consolidated in the “CSE” table already connect the records sought in Part (1) of Plaintiffs’ operative FOIA request, Mr. Gibney is wrong to the extent that he suggests that identifying these records would create difficulties.

Meanwhile, the second set of records that Plaintiffs seek consists of datapoints that are directly or indirectly linked to any person who was “apprehended pursuant to a CBP ‘encounter’ in or after Fiscal Year 2020.” Dkt. 40-7 at 2. When CBP encounters an individual, it “transmit[s] biographic information” about that individual “to EID.” DHS, *Privacy Impact Assessment for the CBP Portal (e3) to EID/IDENT* at 1 (Aug. 2, 2021), <https://tinyurl.com/3pjucrr7>. It then retains the ability to pull encounter-by-encounter data back out of the EID, which it does monthly for reporting purposes. CBP, *Nationwide Encounters* (last updated Oct. 22, 2024) (linking to spreadsheets that contain information about each CBP encounter in a given month), <https://tinyurl.com/yfuptrrw>; see also CBP, *Nationwide Encounters Data Dictionary* (Sept. 2023) (listing the EID as a source of the data in the *Nationwide Encounters* datasets), <https://tinyurl.com/ypa6p4zj>. And the EID contains “unique identifier[s]” for civilians that correspond to “the CBP encounter[s]” during which they were apprehended. Long Decl. Exh. M at 3. Mr. Gibney’s contention that identifying CBP encounters within the EID would require a new “reporting methodology” that would involve “extensive work to design, develop, and test” is therefore wrong. Gibney Decl. ¶ 47. The list of CBP encounters needed to identify the records that are responsive to Part (2) of Plaintiffs’ operative FOIA request already exists. And to the extent that ICE claims that it lacks access to CBP’s list, its argument underscores why Plaintiffs’ request was properly directed to *both* ICE and CBP.

The remaining portion of Plaintiffs' FOIA request does not seek records that are linked to specific individuals at all. It seeks only "code files, lookup tables, or other records" that are built into the EID and that provide a plain-English description of any codes that are used in the records produced pursuant to Parts (1) and (2). *See* Dkt. 40-7 at 2. Mr. Gibney speculates that ICE might "need to expend additional resources" in producing records that are responsive to Part (3) "to the extent" that Plaintiffs seek records "beyond how ... [they] appear in the EID." Gibney Decl. ¶ 48. But as explained above, Plaintiffs have always sought responsive records exactly as they appear within the EID itself. Mr. Gibney's suggestion that producing code translations in some *other* format could require additional work is irrelevant.

Finally, beyond grossly overstating the difficulty ICE would face in locating the records that Plaintiffs seek, Mr. Gibney overstates the burden involved in transmitting them. Assuming that the responsive records would amount to about 3.75 Terabytes of data, Mr. Gibney estimates that it would take "20+ days" to upload the data into the SecureRelease Portal that ICE "typically" uses to deliver documents to FOIA requesters. *Id.* ¶¶ 52–53. During this time, Mr. Gibney claims, "someone would need to be logged in and monitoring the upload" at all times, and the process could cause the SecureRelease Portal to experience delays, thereby inconveniencing other FOIA requesters. *Id.* ¶ 53. Mr. Gibney, though, admits that he "do[es] not have ... much personal experience with the actual delivery of data to FOIA requesters." *Id.* Plaintiffs, on the other hand, have decades' worth of experience with ICE's FOIA productions, some of which have been extremely large. *See, e.g.*, Long Decl. ¶¶ 23–24 (describing a FOIA release through the SecureRelease Portal that contained over 1.8 million records). Moreover, ICE sometimes makes FOIA productions on digital storage media, and not through the SecureRelease Portal, *see id.* ¶ 21, thus obviating Mr. Gibney's concerns about degrading the Portal's

performance during an upload.<sup>5</sup> And despite Mr. Gibney’s insinuation that 3.75 Terabytes is an inherently unmanageable amount of data, a production of that size would fit easily on a portable hard drive that is available online for \$100 or less. *See Amazon.com, Seagate 4TB Enterprise Capacity HDD,* [\*https://tinyurl.com/5c2knnyya\*](https://tinyurl.com/5c2knnyya) (selling a 4-Terabyte hard drive that weighs 1.54 pounds for \$99.99). What is more, as explained above, *see supra* Part I.A.1, Plaintiffs do not ask to have all responsive records compiled into a single aggregated report and produced at once. Mr. Gibney does not explain why producing the EID tables that are responsive to Plaintiffs’ request a few at a time, on a rolling basis, would require any unusual expenditure of bandwidth.

Given the numerous disputed facts that underlie Mr. Gibney’s contention that complying with Plaintiffs’ FOIA request would be unduly burdensome, a factfinder could easily discredit his analysis. ICE has therefore not carried its summary judgment burden on this issue.

### **3. ICE’s burden arguments do not justify its failure to produce *any* responsive records.**

Even setting aside the numerous other flaws in Mr. Gibney’s declaration, his estimate that it would take 8,360 hours to produce *all* of the records that Plaintiffs seek does not address whether *some* responsive records could feasibly be produced. This omission creates another basis for rejecting ICE’s bid for summary judgment on burdensomeness grounds.

Under FOIA, “[a]n agency shall … consider whether partial disclosure of information is possible whenever the agency determines that a full disclosure of a requested record is not possible.” 5 U.S.C. § 552(a)(8)(A)(ii)(I); *see ACLU Immigrants’ Rights Project*, 58 F.4th at 654 (recognizing that the government bears the burden of demonstrating the inability to produce

---

<sup>5</sup> Other government agencies, including components of the U.S. Department of Justice, regularly transfer large files through specialized web platforms. *See, e.g., DOJ, FY 2022 Annual Performance Report* at 123 (2023), [\*https://tinyurl.com/7xrsjmvu\*](https://tinyurl.com/7xrsjmvu) (explaining that the Bureau of Prisons “has streamlined data transfer protocol by using Justice Enterprise Files Sharing (JEFS) to transmit large data files in response to external inquiries”).

segregable portions of requested records). Accordingly, even if a factfinder credits Mr. Gibney’s disputed claim that it would be unduly burdensome for ICE to comply fully with Plaintiffs’ FOIA request, the appropriate result would be for this Court to “craft remedies” that minimize the burden and to “work with the parties to establish realistic timelines for compliance.” *N.Y. Legal Assistance Grp. v. BIA*, 987 F.3d 207, 225 (2d Cir. 2021). In one recent FOIA case, for example, the Second Circuit responded to an agency’s claim that “it would take four employees working full-time nearly seven years” to prepare and release the requested records—750,000 prior agency opinions—by noting that the district court could prioritize the release of more recent opinions and “set[] a timetable for making older decisions available.” *Id.*

Here, ICE has presented no evidence that it has complied with its statutory obligation to consider partial production. Although Mr. Gibney claims to have “no existing EID queries that would produce data *fully responsive*” to Parts (1) or (2) of Plaintiffs’ FOIA request, Gibney Decl. ¶ 41 (emphasis added), the evidence shows that ICE and CBP’s existing capabilities enable them to easily extract a large portion of the case-by-case data that Plaintiffs seek from the EID. *See supra* pp. 10–11. And as the Second Circuit recently noted, “the few courts to have considered the question have concluded that it is not unduly burdensome to require agencies already possessing computer capabilities to acquire software or to craft new computer queries to be able to retrieve responsive electronic records from their databases.” *ACLU Immigrants’ Rights Project*, 58 F.4th at 662; *see also* 6 C.F.R. § 5.4(i)(2)(ii) (explaining that query-building for FOIA purposes is “business as usual”). Because Mr. Gibney’s declaration does not explain whether *any* records can be produced without requiring the laborious steps that he claims would be necessary for a full production, it is insufficient to establish that *no* records can feasibly be produced in response to Plaintiffs’ FOIA request.

**B. ICE has not shown that FOIA exemptions relieve it of its obligation to produce any responsive records.**

ICE next argues that it need not produce any records because certain data that falls within the scope of Plaintiffs' FOIA request is exempt from disclosure. When an agency asserts that a FOIA exemption applies, “[t]he agency … bears the burden of proof, and all doubts as to the applicability of the exemption must be resolved in favor of disclosure.” *Osen LLC*, 969 F.3d at 114 (quoting *Wilner v. NSA*, 592 F.3d 60, 69 (2d Cir. 2009)). Moreover, as a result of FOIA amendments that Congress enacted in 2016 out of concern that the government was overusing FOIA exemptions, “[a]pplicability of a FOIA exemption is … necessary—but no longer sufficient—for an agency to withhold … requested information.” *Seife*, 43 F.4th at 235. Even after an agency establishes that an exemption applies, FOIA requires the agency to show further that it “reasonably foresees that disclosure would harm an interest protected by an exemption.”<sup>6</sup> 5 U.S.C. § 552(a)(8)(A)(i)(I). Even then, the agency must produce “[a]ny reasonably segregable portion of a record … after deletion of the portions which are exempt.” *Id.* § 552(b).

Here, ICE contends that portions of the requested records fall within various exemptions because their release could compromise personal privacy or safety (Exemptions 7(C), 6, and 7(F)); adversely affect law-enforcement operations, particularly by increasing the risk of a cyberattack (Exemptions 7(E) and 7(A)); or reveal statutorily protected material (Exemption 3). ICE has not shown beyond genuine dispute that releasing the records would realistically create any of these claimed concerns, especially if the records are appropriately redacted.

---

<sup>6</sup> This additional requirement does not apply where the government claims that the records withheld are exempted from disclosure by statute. See 5 U.S.C. § 552(a)(8)(B).

**1. ICE has not shown that personal privacy and safety concerns justify withholding all requested records under Exemptions 7(C), 6, and 7(F).**

Relying principally on the declaration of Heather Lynch, ICE contends that Plaintiffs' FOIA request seeks records that could permit the re-identification of the individuals to whom EID records pertain and could therefore compromise those individuals' personal privacy or safety. Accordingly, ICE claims that *all* of the requested records are exempt from disclosure under Exemption 7(C), which exempts law-enforcement records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy," 5 U.S.C. § 552(b)(7)(C), Exemption 6, which exempts "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," *id.* § 552(b)(6), and Exemption 7(F), which exempts law-enforcement records that "could reasonably be expected to endanger the life or physical safety of any individual," *id.* § 552(b)(7)(F). None of these exemptions justify ICE's withholding of all responsive records.

**Exemption 7(C).** ICE first argues that the privacy of individuals whose information is contained in the EID could be subject to unwarranted invasion if the requested records were produced. Dkt. 40-1 at 20–24. But while the "privacy interests protected by the exemptions to FOIA are broadly construed," FOIA requires disclosure of records that implicate those interests "if the requestor can show that revelation of the contents of the requested [records] would serve the public interest." *Associated Press v. DOJ*, 549 F.3d 62, 65–66 (2d Cir. 2008) (per curiam). To determine whether Exemption 7(C) shields records from disclosure, then, a court must balance the risk to personal privacy against "the extent to which disclosure would serve the core purpose of the FOIA, which is contribut[ing] significantly to public understanding of the operations or activities of the government." *Id.* at 66 (alteration in original; quoting *U.S. Dep't of Def. v. FLRA*, 510 U.S. 487, 495 (1994)). Here, ICE fails to explain why redaction cannot

adequately address any privacy concerns, overstates the amount of sensitive personal information in the EID in the first place, and entirely neglects to address the public interest in disclosure.

The core privacy concern addressed in Ms. Lynch's declaration, on which ICE chiefly relies, is that the records sought would "present[] an unacceptable risk of exposing individuals' identities" if released. Lynch Decl. ¶ 2. But while ICE asserts that the D.C. Circuit has held that "identities contained in law enforcement records are categorically protected," Dkt. 40-1 at 21 (citing *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1206 (D.C. Cir. 1991)), *SafeCard*'s actual language is more precise. That case holds that "unless access to the *names and addresses* of private individuals appearing in files within the ambit of Exception 7(C) is necessary in order to confirm or refute compelling evidence that the agency is engaged in illegal activity, such information is exempt from disclosure." 926 F.2d at 1206 (emphasis added). Here, Plaintiffs have not challenged ICE's decision to redact any directly identifying information from released records. Rather, ICE is preemptively asserting that it need not release any records at all because a highly motivated, "technically savvy third party" could theoretically combine *indirect* identifiers in the EID with other "publicly available information" to reverse-engineer an individual's identity, "even [if] direct identifiers have been stripped" from the records. Lynch Decl. ¶ 30.

ICE cites no authority to support this sweeping expansion of Exemption 7(C). It briefly alludes to *Weisberg v. DOJ*, 745 F.2d 1476 (D.C. Cir. 1984), for the proposition that "privacy interests remain even where other information may allow the public to 'piece together' an individual's identity." Dkt. 40-1 at 21. But *Weisberg*, like *SafeCard*, involved a challenge to an agency's decision to redact the *names* of individuals mentioned in the records it was producing. See 745 F.2d at 1491. If anything, *Weisberg* highlights the extremity of ICE's position here. In *Weisberg*, the D.C. Circuit held that the FBI had properly redacted two informants' names from

its investigation files, although the plaintiff was able to “piece together” the informants’ identities based on other sources. *Id.* Under ICE’s theory, the risk of the informants’ re-identification would have allowed the government to withhold the *entire file*.

But even granting ICE the dubious proposition that Exemption 7(C) guards against the risk that a malevolent actor might wade through reams of anonymized data to identify a specific person, FOIA requires “agencies and courts to differentiate among the contents of a document” and to “divide the record into parts that are exempt and parts that are not exempt.” *FBI v. Abramson*, 456 U.S. 615, 626 (1982). And ICE carries the burden of demonstrating that the exempt portions cannot reasonably be segregated from the nonexempt records. *See ACLU Immigrants’ Rights Project*, 58 F.4th at 654. ICE cannot carry this burden.

According to Ms. Lynch, the privacy risks of re-identification are acute because the EID contains sensitive personal information (SPI), such as transgender status and health information, Lynch Decl. ¶ 16, the disclosure of which “could result in discrimination or impact the [re-identified] individual’s rights, safety, opportunities, and social or psychological well-being,” *id.* ¶ 7. Ms. Lynch identifies several fields that could compromise privacy if re-identification were successful. *See, e.g., id.* ¶¶ 16–28 (stating that the EID contains information on health conditions, physical characteristics, gang affiliation, and criminal history). The fact that Ms. Lynch is able to identify the particular fields of information that supposedly raise privacy concerns, however, belies the claim that ICE is incapable of identifying and redacting the portions of the EID that ICE claims are exempt. ICE vaguely claims that “nonexempt information is ‘inextricably intertwined’ with exempt information,” Dkt. 40-1 at 34 (quoting *Mead Data Central, Inc. v. U.S. Dep’t of Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977)), but the EID is divided into discrete and easily segregable tables, and information within each table is organized into a series of fields,

each of which contains a clearly defined category of information. *See* Long Decl. ¶ 10. Some tables—like the “CSE” table—contain no fields that reveal any sort of personally identifying information. *Id.* ¶ 16 & Exh. M. And if a table contains some fields that could reveal such information, ICE can redact those fields. *See, e.g.*, Long Decl. ¶ 19 & Exh. O (noting redaction of the “Date of Birth” column in released records to reduce the risk of re-identification).

Indeed, ICE has not even attempted to make the showing required by *Mead Data Central*, the case that it cites for the proposition that an agency need not attempt to segregate nonexempt records when they are inextricably intertwined with exempt records. Emphasizing that “segregability depends entirely on what information is in a document and how it is presented,” *Mead Data Central* holds that an agency that claims an inability to segregate exempt and nonexempt records “should … describe what proportion of the information in a document is non-exempt and how that material is dispersed throughout the document.” 566 F.2d at 261; *see Hopkins v. HUD*, 929 F.2d 81, 85 (2d Cir. 1991) (holding that summary judgment for the agency was improper where the agency had “only asserted in a conclusory fashion” that nonexempt factual information in the requested records was “‘inextricably intertwined’ with the [records’] privileged opinions and recommendations”). ICE has not explained why the sort of field-by-field redaction that it has performed in the past would be infeasible or impractical here.

The only justification that ICE offers for refusing to make any effort to segregate the portions of the EID that ICE believes can be withheld under Exemption 7(C) is that certain re-identification risks could remain “even after ICE removes direct identifying information.” Dkt. 40-1 at 35. But nothing prevents ICE from asserting the right to redact *indirect* identifiers—such as “gender, birth year, occupation, or country of origin”—that ICE now claims to view as posing a threat to privacy, *id.* at 37, despite having released such information in the past, *see* Long Decl.

¶¶ 18–24 & Exhs. P, R, T. Plaintiffs have already consented to the redaction of “any free-format fields or, in other words, fields that contain potentially unique individualized content entered into each cell, as distinct from standardized-content fields that allow only standardized entries (such as dates, times, numbers, codes, or categories).” Dkt. 40-7 at 2. Although Plaintiffs cannot opine in the abstract on the propriety of any other redactions ICE might hypothetically elect to make, ICE has control over what data it releases and what data it redacts as part of a FOIA production (subject, of course, to any legally supported challenges to ICE’s redaction decisions). Put simply, ICE has offered no support for its apparent view that it need not produce *any* responsive records simply because it believes that those records must be heavily redacted.

Insofar as Ms. Lynch implies that the quantity of information in the EID renders re-identification inevitable notwithstanding proper redaction, her insinuation rests on disputed facts. Ms. Lynch claims that the EID “contains approximately 12,000 data fields directly or indirectly linked to a migrant’s case,” Lynch Decl. ¶ 5, spread “across roughly 1,000 tables,” *id.* ¶ 15, but these numbers are simply wrong. As explained above, *see supra* p. 9, the EID contains at most 399 data tables, not 1,000. And a recently released list of all of the EID’s tables and data fields reflects only 9,279 total fields, many of which appear in code tables (not data tables). *See* Long Decl. ¶¶ 11–14; *see also supra* p. 9 n.3 (explaining the distinction between code tables and data tables). Ms. Lynch therefore has no basis for claiming that each case is directly or indirectly linked to 12,000 data fields. More importantly, despite referring to the SPI contained in the EID as “extensive,” Lynch Decl. ¶ 5, Ms. Lynch does not offer even a ballpark figure as to what proportion of the EID’s fields contain such information. As it happens, the evidence suggests that most of the EID’s fields relate to the *government’s* activities and not to the identities or characteristics of individuals. *See, e.g.,* Long Decl. ¶ 24 & Exh. T. For example, the “CSE”

table—which forms the basis for Part (1) of Plaintiffs’ request—contains no personal information at all. *See Long Decl.* ¶ 16 & Exh. M.

In any event, evidence shows that ICE *does* believe that large quantities of person-by-person data can be released without unduly compromising personal privacy. After all, ICE regularly releases such data. *See, e.g.*, Long Decl. ¶¶ 18–24 & Exhs. P, R, T. Even during the course of this litigation, ICE released case-by-case data associated with nearly 1.8 million noncitizens, with over 120 unredacted fields of information provided in connection with each case. Long Decl. ¶¶ 23–24 & Exh. T. These fields included information such as the noncitizen’s gender, citizenship country, birth country, birth year, race, ethnicity, and criminal history. Long Decl. ¶ 24 & Exh. T. Indeed, ICE regularly *directly* identifies the subjects of its enforcement actions. *See, e.g.*, ICE, *ERO Removes Noncitizen Wanted for Homicide to El Salvador* (Oct. 18, 2024), <https://tinyurl.com/2zb8fpux> (announcing removal of “Gustavo Adolfo Rivas Munoz, a citizen of El Salvador,” and publishing Mr. Munoz’s photographs and criminal history); ICE, *ERO Boston Arrests Brazilian National Charged with Drug, Firearms, Ammunition Crimes in Martha’s Vineyard* (Oct. 4, 2024), <https://tinyurl.com/48zdt892> (announcing arrest of Gustavo Augusto Mroczkoski, “a 28-year-old Brazilian national charged with drug, firearms and ammunition crimes,” and publishing Mr. Mroczkoski’s photograph).

ICE’s past and current practice in this regard offers a strong basis for a factfinder to discredit ICE’s present contention that no level of redaction could reduce the risk of re-identification to an acceptable level. In Ms. Lynch’s telling, malevolent actors can *already* deduce the identity of the individuals described in the public releases that ICE makes as a matter of course. *Compare Lynch Decl.* ¶ 44 (warning that individuals could be re-identified “in just under an hour” by comparing detention information in the EID to “local city and state online

public arrest records”), *with* Long Decl. Exh. T (noting ICE’s release of unredacted details of, among other things, “Latest Detention Stay Book In Date and Time” and “Latest Stay Earliest Detention Facility”). But ICE apparently either views the hypothetical risk that an ambitious wrongdoer will sift through voluminous database entries to piece together a specific individual’s identity as unrealistic or believes that its redaction decisions have been sufficient to ensure that re-identification would not reveal sensitive information if it were to occur. Certainly, ICE has produced no evidence that its prior releases have created any non-theoretical privacy risk.

Meanwhile, as against ICE’s unsubstantiated fear that a bad actor might be motivated to work backwards from a large dataset of anonymous removal cases or CBP encounters to attempt to identify and learn some damaging (yet somehow unredacted) fact about a particular individual, ICE does not even attempt to address the public interest in access to the requested records. *See Associated Press v. U.S. Dep’t of Def.*, 554 F.3d 274, 285 (2d Cir. 2009) (explaining that the application of Exemption 7(C) requires consideration of the degree to which production of the requested records would further “the citizens’ right to be informed about what their government is up to” (quoting *Ray*, 502 U.S. at 177)). As explained above, *see supra* pp. 20–21, the bulk of the information in the EID appears to concern ICE’s activities, and Plaintiffs’ motivation for seeking the requested records is to expose those activities to public view. The demonstrated value of Plaintiffs’ work is high, and numerous institutions rely on the data that Plaintiffs gather and analyze. *See* Long Decl. ¶¶ 3–4. ICE’s speculative hypotheticals cannot justify the certain and concrete harm of withholding information about the government’s immigration enforcement activities from a public that has a strong interest in demanding accountability.

**Exemption 6.** ICE’s claim that the requested records are covered by Exemption 6 relies entirely on ICE’s Exemption 7(C) analysis. Dkt. 40-1 at 31. Unlike Exemption 7(C), however, “[a]n invasion of more than a *de minimis* privacy interest protected by Exemption 6 must be shown to be ‘*clearly* unwarranted’ in order to prevail over the public interest in disclosure.” *FLRA v. U.S. Dep’t of Veterans Affs.*, 958 F.2d 503, 510 (2d Cir. 1992) (emphasis added). Accordingly, “the government’s burden in establishing the required invasion of privacy” under Exemption 6 “is heavier than the burden in establishing invasion of privacy under Exemption 7(C).” *Associated Press v. U.S. Dep’t of Def.*, 554 F.3d 274, 291 (2d Cir. 2009); *see Cook v. Nat'l Archives & Records Admin.*, 758 F.3d 168, 176 n.8 (2d Cir. 2014) (observing that “Exemption 7 affords a greater degree of privacy protection than Exemption 6”). Because ICE cannot carry its burden under Exemption 7(C), it necessarily cannot carry its heavier burden under Exemption 6.

**Exemption 7(F).** ICE’s argument that Exemption 7(F) authorizes it to withhold all of the requested records fails for similar reasons. Exemption 7(F) requires an agency to show “some nexus between disclosure and possible harm” and to show that “deletions were narrowly made to avert the possibility of such harm.” *Petrucelli v. DOJ*, 51 F. Supp. 3d 142, 172 (D.D.C. 2014) (quoting *Antonelli v. BOP*, 623 F. Supp. 2d 55, 58 (D.D.C. 2009)). An agency cannot rely on “conclusory assertions that disclosure will increase the chances that third parties will be harmed in some way,” and “unsupported speculation cannot serve as a justification for withholding information under Exemption 7(F).” *Long v. DOJ*, 450 F. Supp. 2d 42, 80 (D.D.C. 2006). Rather, the agency must “reasonably foresee[]” that harm could occur. 5 U.S.C. § 552(a)(8)(A)(i)(I).

As with Exemption 7(C), ICE focuses its argument on the risk of identification. And as with Exemption 7(C), ICE’s past release of vast amounts of case-by-case data related to millions

of individuals casts doubt on whether ICE genuinely sees a realistic risk. And again, as with Exemption 7(C), ICE cannot show why targeted redaction would fail to avert the risk of harm. Indeed, ICE’s own examples illustrate the point. ICE argues that a noncitizen could face a risk of discrimination if the noncitizen is re-identified and associated with a “vulnerability code” that ICE assigns to members of certain populations. Dkt. 40-1 at 29. Redacting the “vulnerability code” would presumably alleviate this concern. Similarly, ICE points to concerns related to disclosing information about a noncitizen’s “LGBT identity” or medical conditions, *id.* at 30, but it fails to explain why this sort of sensitive information could not be redacted if necessary. In short, just as ICE cannot show that withholding all of the requested records is necessary to protect personal privacy, it cannot show that doing so is necessary to protect physical safety.<sup>7</sup>

**2. ICE has not shown that law-enforcement concerns justify withholding all requested records under Exemptions 7(E) and 7(A).**

Contending that releasing any requested records could impede law enforcement, ICE invokes Exemption 7(E), which permits withholding of law-enforcement records that “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law,” 5 U.S.C. § 552(b)(7)(E), and Exemption 7(A), which permits withholding of law-enforcement records that “could reasonably be expected to interfere with enforcement proceedings,” *id.* § 552(b)(7)(A). Neither exemption justifies ICE’s wholesale refusal to produce any records.

---

<sup>7</sup> ICE also briefly argues that a cyberattack on the EID could endanger physical safety if it caused law-enforcement personnel to release violent criminals. Dkt. 40-1 at 30. ICE’s invocation of this far-fetched scenario does not establish that releasing the requested records would lead to reasonably foreseeable physical dangers—especially because, as explained below, ICE has not demonstrated that disclosure of the requested records would increase the likelihood of a cyberattack on the EID. *See infra* pp. 26–30.

**Exemption 7(E).** ICE maintains that Exemption 7(E) justifies withholding all requested records, but although ICE argues that this exemption “protect[s] database information which, if disclosed, would undermine law enforcement efforts,” Dkt. 40-1 at 24, neither ICE nor the declaration of Nate Fontaine, on which ICE relies, attempts to articulate—even in the most general terms—what sort of law-enforcement “techniques and procedures” or “guidelines” risk being “disclose[d],” 5 U.S.C. § 552(b)(7)(E). *See* Fontaine Decl. ¶ 22 (referring generally to the EID’s “data related to law enforcement techniques and procedures”); *id.* ¶ 28 (imagining a hypothetical situation in which ICE “developed a new law enforcement technique or procedure related to arrests” and supposing that the EID could “reflect the new [hypothetical] technique or procedure” in some unspecified way). Right out of the gate, then, ICE has failed to establish an essential predicate for Exemption 7(E)’s application.

The closest that ICE comes to asserting that the requested records would reveal law-enforcement techniques, procedures, or guidelines centers on Mr. Fontaine’s testimony regarding “metadata” that could reveal changes to the EID’s structure and contents over time.<sup>8</sup> Dkt. 40-1 at 27. Mr. Fontaine notes that ICE has previously released versions of the EID’s “data dictionary” (a document that lists the names of the tables and fields contained in the EID) and “Code Lookups” that translate codes used in the data tables into plain English (for example, by indicating that the abbreviation “VA” denotes “Virginia”). Fontaine Decl. ¶ 27; *see* Gibney Decl. ¶ 10 (explaining the EID’s use of coded values); Long Decl. ¶¶ 11, 13 (detailing ICE’s recent release of the EID’s data dictionary and code tables). Mr. Fontaine does not identify any adverse impact on law enforcement that these releases have had. Instead, he claims that release of the

---

<sup>8</sup> ICE also briefly reprises its claim that the requested records contain “highly sensitive personal information” about witnesses. Dkt. 40-1 at 26. ICE does not attempt to explain how this information relates to law-enforcement techniques, procedures, or guidelines, and as explained above, *see supra* pp. 18–22, ICE has not shown why sensitive information cannot be redacted.

*current* versions would allow bad actors to compare these versions to prior versions, identify “the differences between … versions,” and so learn which (unspecified) law-enforcement techniques and procedures are “the latest and least publicly known.” Fontaine Decl. ¶ 28.

Mr. Fontaine offers no basis for this vague and speculative concern. For one thing, the EID’s data dictionaries—past and present—exist outside the EID itself and so are not within the scope of Plaintiffs’ request in the first place. As for code translations, they are a standard component of any database and are essential to interpreting data that would otherwise be unintelligible. For example, without the information in the code table that is attached as an exhibit to the declaration of Susan B. Long, somebody examining the EID would not know that “TCO” means “Transferred Case Officer” when that abbreviation appears in certain data tables. Long Decl. Exh. L; *see also, e.g.*, Long Decl. Exh. M at 1 (ICE release indicating that, when used in the field “CSE\_CEC\_DC,” the number “1” refers to “ICE”). As a result of the necessary role that these translations play, ICE regularly releases them when it releases data fields. *See* Long Decl. ¶ 25. Indeed, ICE has already produced many of the EID’s code tables in another litigation. *Id.* ¶ 13. And an ICE witness conceded in that case that “codes and code translations within certain code lookup tables c[an] be released without creating an unacceptable risk to the security of the EID.” *Long v. ICE*, 464 F. Supp. 3d 409, 424 (D.D.C. 2020). ICE also offers no explanation why its concededly benign code translations suddenly create a risk to law enforcement if the recency of their creation or alteration can be determined by comparing them to prior versions. After all, the EID data that ICE has publicly released contains unredacted fields that state when database codes were created and last modified. *See* Long Decl. ¶ 13 & Exh. L.

ICE’s chief Exemption 7(E) argument is not that honoring Plaintiffs’ FOIA request would *itself* reveal law-enforcement techniques, procedures, or guidelines, but rather that

producing the requested records would “increase the risk of a cyberattack on the EID,” which *in turn* could lead to the disclosure of such information, along with other harms. Dkt. 40-1 at 26. This theory cannot withstand scrutiny. ICE’s sole evidence—Mr. Fontaine’s declaration—says vanishingly little about why ICE believes that producing the requested records would increase the risk of such an attack. Instead, Mr. Fontaine emphasizes the negative consequences that could arise from unauthorized access to the EID, *see, e.g.*, Fontaine Decl. ¶¶ 5–8, 19–25, catalogues other cyberattacks that have occurred in other contexts, *see, e.g., id.* ¶¶ 12–14, 36–39, and speaks generally about the government’s response to the threat of cyberattacks, *see, e.g., id.* ¶¶ 15–18. Certainly, Plaintiffs do not dispute that a hacker who somehow breached the “sustained and sophisticated defense[s]” that ICE has erected to prevent external users from gaining access to its network, *id.* ¶ 5, could do harm once inside. But Mr. Fontaine barely attempts to claim that knowing the contents of the EID would aid a bad actor in *accessing* the EID. *See EID Privacy Impact Assessment* at 13 (explaining that “[a]uthentication and role-based user access requirements ensure that users only can access or change EID information that is appropriate for their official duties” and that “[t]he effectiveness of authentication and security protections are verified through audits of system operation and usage”). Mr. Fontaine briefly contends that knowing about the EID’s structure could allow a would-be cybercriminal to “craft highly targeted emails or communications aimed at tricking employees into giving up sensitive information or credentials,” Fontaine Decl. ¶ 37, but this objection could be raised with *any* FOIA request, given that *any* information about government operations could enable a sophisticated impersonator to sound more credible.

Mr. Fontaine’s cybersecurity concerns thus rest principally on the theory that disclosing “certain details of the EID data structure” would assist a bad actor in carrying out a cyberattack

after the bad actor has gained unlawful access to ICE’s systems. *Id.* ¶ 30. The flaw in this theory is self-evident: Once a hacker is already unlawfully inside the EID, the hacker will have access to “details of the EID data structure,” *id.*, whether or not ICE has previously released them. Ultimately, then, Mr. Fontaine is reduced to contending that a “[c]ybersecurity threat actor[]” could use released FOIA records to “conduct extensive research” on the EID so as to conduct a more efficient attack by building an advance model of a “malicious quer[y]” that the actor could run after somehow finding a successful way to hack into ICE’s system. *Id.* ¶¶ 34–35. He fails, however, to identify any requested records that credibly present this concern. He first objects to the disclosure of “relational information” such as “primary keys” and “foreign keys,” which could reveal how the EID’s tables are connected to one another. *Id.* ¶¶ 33, 35. But ICE routinely releases this sort of information. Cf. *ACLU Immigrants’ Rights Project*, 58 F.4th at 654–55 (requiring ICE to preserve relational information in a recent FOIA release). As noted above, ICE has released many of the EID’s code tables, thus enabling the public to see how a vast quantity of primary keys (the codes listed in the code tables) connect to a vast quantity of foreign keys (fields in data tables that use the coded values). Of particular relevance here, ICE appears to have already released all of the primary and foreign keys in the “CSE” table, upon which Part (1) of Plaintiffs’ FOIA request focuses. See Long Decl. ¶ 16 & Exh. M. Mr. Fontaine does not explain why the release of *additional* foreign and primary key information would provide a would-be hacker any incremental advantage.

While Mr. Fontaine also points to the release of “references to [ICE’s] organizational structure” as potentially problematic, Fontaine Decl. ¶ 30, this information, too, is publicly available. ICE, *Organizational Structure* (last updated Aug. 20, 2024), <https://tinyurl.com/5ftn3zkp>. Meanwhile, Mr. Fontaine’s concern about the release of “data type descriptions” that

would reveal, for example, that “certain fields only accept[] numeric data,” Fontaine Decl. ¶ 38, is no more persuasive. These descriptions reveal nothing that cannot already be inferred from the underlying data itself. For example, an “age” field will contain a number, while an “apprehension date” field will contain a date. Anybody who examines the extensive EID records that ICE regularly releases to the public, *see supra* pp. 21–22, can easily determine whether particular fields are populated with alphanumeric text strings, coded terms, standardized dates or times, binary “yes/no” indications, or the like. In short, Mr. Fontaine does not explain why reasonably foreseeable harm would arise from stating what is already plainly apparent.

What is more, Mr. Fontaine’s concerns focus on material within the EID that he appears to concede could “be redacted.” Fontaine Decl. ¶ 29. Indeed, ICE’s argument that it cannot reasonably segregate exempt records from nonexempt records addresses only Ms. Lynch’s re-identification theory and is conspicuously silent on Mr. Fontaine’s cybersecurity theory. *See* Dkt. 40-1 at 34–38. This silence is unsurprising. ICE has previously acknowledged that release of the underlying *data* contained in the EID—as distinct from the metadata that describes how the EID is structured—creates no cybersecurity threat. *See* Sansone Decl. Exh. D at 62 (ICE witness’s testimony that “the contents of [ICE’s] database are subject to FOIA” and that the “release of information about what’s in [the] database” does not necessarily “constitute a threat”) & Exh. G ¶ 12 (ICE declaration attesting to a request for case-by-case data containing 54 data fields for each case that ICE disclosed “without releasing … database information capable of compromising the system”).

Even within the category of metadata, ICE cannot establish that *all* information about the EID’s structure creates a cybersecurity threat, such that *no* records on that subject can be produced. ICE has previously admitted as much. *See* Sansone Decl. Exh. D at 63 (ICE witness’s

admission that disclosing “the actual name of a field” from an ICE database would not necessarily “create an unacceptable risk”). ICE’s past practices confirm as much. *See supra* pp. 21–22. And the U.S. District Court for the District of Columbia held as much following a two-day evidentiary hearing during which ICE had the opportunity to make an *in camera* presentation of its cybersecurity concerns. *See Long*, 464 F. Supp. 3d at 425 (holding that the release of various metadata, including “field and table names, codes, code translations, and code lookup tables,” does not create a categorical risk to law-enforcement interests). To the extent that Mr. Fontaine’s asserted cybersecurity concerns have any basis in reality, ICE’s duty under FOIA is to determine what can properly be released and to release it. ICE has not even attempted to do so.

**Exemption 7(A).** Exemption 7(A)’s “principal purpose” is to “prevent disclosures which might prematurely reveal the government’s cases in court, its evidence and strategies, or the nature, scope, direction, and focus of its investigations, and thereby enable suspects to establish defenses or fraudulent alibis or to destroy or alter evidence.” *Maydak v. DOJ*, 218 F.3d 760, 762 (D.C. Cir. 2000). ICE urges this Court to make a “generic determination[]” that releasing the requested records would “generally interfere with enforcement proceedings,” Dkt. 40-1 at 18 (quoting *Lazaridis v. U.S. Dep’t of State*, 934 F. Supp. 2d 21, 37 (D.D.C. 2013)), but it is ICE’s burden to establish a reasonably foreseeable prospect that disclosure of the records will “cause some distinct harm to [a] pending or imminent enforcement proceeding or investigation,” *Lazaridis*, 934 F. Supp. 2d at 37; *see 5 U.S.C. § 552(a)(8)(A)(i)(I)*. ICE’s vague allusions to unspecified risks are insufficient to carry this burden.

Citing no evidence, ICE first contends broadly that producing “demographic information regarding those who are subject to removal proceedings” could reveal law-enforcement methods or “cause harm on a broader level” by disclosing unspecified aspects of “CBP encounters and

ICE removal proceedings.” Dkt. 40-1 at 18–19. As explained above, however, ICE regularly discloses vast swaths of data about the targets of its enforcement actions. *See supra* pp. 21–22. CBP does the same. *See, e.g.*, CBP, *CBP Office of Field Operations Statistics* (last updated Nov. 4, 2024), <https://tinyurl.com/fnrbejj5> (linking to multiple spreadsheets like “OFO Inadmissibles August to September 2024,” which contains demographic information associated with the enforcement targets of over 180,000 CBP encounters). ICE never explains what categories of demographic information above and beyond those that it already releases would raise concerns if disclosed. *Cf. Maydak*, 218 F.3d at 765 (explaining that the government “satisfies its burden of proof under Exemption 7(A) by grouping documents in categories” and presenting justifications for “withholding the documents in each category”). And ICE offers no “specific information” about what those concerns might be. *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1114 (D.C. Cir. 2007); *see Citizens for Responsibility & Ethics in Wash. v. DOJ*, 746 F.3d 1082, 1098 (D.C. Cir. 2014) (hereafter, *CREW*) (“[I]t is not sufficient for the agency to simply assert that disclosure will interfere with enforcement proceedings; ‘it must rather demonstrate *how* disclosure’ will do so.” (quoting *Sussman*, 494 F.3d at 1114)).

In addition, ICE claims that releasing the requested records could “increase the risk of a cyberattack on the EID,” which could in turn compromise enforcement proceedings that rely on the integrity of the EID’s data. Dkt. 40-1 at 19. But while ICE cites the declaration of Nate Fontaine to support its reasonable contention that a cyberattack could have negative implications for ICE’s enforcement activities, ICE cites *no* evidence to support the underlying premise of its argument: namely, that producing the requested records will increase the risk of such an attack. As explained above, *see supra* pp. 26–30, this premise is wrong.

Finally, ICE voices concern that disclosing the requested records could create a risk that witnesses and prosecutors could be re-identified and subjected to intimidation. Dkt. 40-1 at 19–20. This argument fails for the same reasons that ICE’s privacy-based arguments fail: As explained above, *see supra* Part I.B.1, ICE offers no evidence that the speculative risk of identification will likely materialize and does not explain why potentially identifying information cannot be redacted. Indeed, ICE offers no evidence regarding how much witness and prosecutor information the EID contains and whether that information is clustered in a limited handful of easily segregable EID tables or fields. Given that ICE bears the burden of showing that any exempt portions of a record cannot reasonably be segregated from nonexempt portions, *ACLU Immigrants’ Rights Project*, 58 F.4th at 654, this omission is fatal to ICE’s argument.

Even if ICE had offered evidence that producing the requested records could interfere with ongoing enforcement proceedings (which it has not), ICE has not shown why it could not release records related to *closed* cases. *See CREW*, 746 F.3d at 1097 (“[R]eliance on Exemption 7(A) may become outdated when the [law-enforcement] proceeding at issue comes to a close.”); *Grand Central P’ship, Inc. v. Cuomo*, 166 F.3d 473, 485 n.5 (2d Cir. 1999) (noting that Exemption 7(A) is “not applicable in the absence of some evidence that ‘enforcement proceedings’ are actually being conducted”). The EID’s “CSE” table, which forms the basis for Part (1) of Plaintiffs’ operative FOIA request, contains a field indicating whether a given case is open. *See* Long Decl. Exh. M at 1 (reflecting a “CSE\_CCDSC\_CD” field that contains “case status[]” information and noting that a case is considered “Active” when that field contains the code “ACT”). Filtering out the cases with an “ACT” status code would produce an easily segregable set of records to which Exemption 7(A) could not conceivably apply.

**3. ICE has not shown that its grab-bag of miscellaneous statutory provisions justifies withholding all requested records under Exemption 3.**

Finally, ICE invokes FOIA’s Exemption 3, which exempts an agency from producing any “matters” that are “specifically exempted from disclosure by statute,” provided that the statute either “requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue” or “establishes particular criteria for withholding or refers to particular types of matters to be withheld.” 5 U.S.C. § 552(b)(3)(A). To carry its burden of establishing that this exemption applies, an agency must show that “(1) the statute invoked qualifies as an Exemption 3 withholding statute, and (2) the materials withheld fall within that statute’s scope.” *Bloomberg L.P. v. U.S. Postal Serv.*, 118 F.4th 307, 315 (2d Cir. 2024) (quoting *Spadaro v. CBP*, 978 F.3d 34, 42 (2d Cir. 2020)). Here, ICE claims that it cannot produce any records from the EID because doing so could “violat[e] another statute,” and it goes on to identify assorted statutory provisions that Plaintiffs’ FOIA request “could implicate.” Dkt. 40-1 at 32.

ICE has patently failed to carry its burden of establishing that any of the requested records fall within Exemption 3—let alone that *all* of them do. ICE offers no analysis of any of the statutes that it cites, and it makes no argument as to why any one of them “qualifies as an Exemption 3 withholding statute.” *Bloomberg*, 118 F.4th at 315. Moreover, despite stating that, “[b]ased on a preliminary review of the EID datapoints,” some unspecified subset of those datapoints “could implicate any number of statutes,” Dkt. 40-1 at 32, ICE draws no connection between any particular EID data and any particular statute. “[M]erely stating that ‘for example’ an exemption might apply is inadequate to raise a FOIA exemption.” *Maydak*, 218 F.3d at 765.

A few examples illustrate the point. Citing “18 U.S.C. § 2510, *et seq.*,” ICE claims that granting Plaintiffs’ FOIA request could violate one of the many statutory provisions that “pertain to law enforcement activities that include wire taps and pen registers.” Dkt. 40-1 at 34. Which

provision? ICE does not say. Where would the violation lie? Silence again. ICE also claims that production of the requested records could violate statutory prohibitions on disclosing certain tax-return information. *Id.* (citing 26 U.S.C. §§ 6103, 6105). Does the EID contain any tax-return information, though? ICE has not claimed as much. Even for those statutes that are potentially more relevant to the EID’s purview, ICE merely quotes statutory text without explaining how it applies. *See, e.g., id.* at 32–33 (quoting 8 U.S.C. § 1367(a)(2)). The fact that a statute may justify withholding some information in some cases does not mean that ICE has shown that the statute justifies withholding *all* requested records in *this* case. Cf. *Project South v. ICE*, No. 1:21-cv-08440, 2024 WL 1116164, at \*9 (S.D.N.Y. Mar. 12, 2024) (holding that 8 U.S.C. § 1367(a)(2), which forbids disclosing information related to certain asylum-seekers, did not justify an Exemption 3 withholding where it was “highly unlikely” that “a third party [could] link the identity of an individual to the details of their asylum claims” based on the records requested).

Furthermore, ICE cannot possibly believe that *no* requested records can be released under FOIA without “violating another statute.” Dkt. 40-1 at 32. Otherwise, ICE has been flouting the law for years by regularly releasing large quantities of EID data. *See supra* pp. 21–22. As with the other claimed exemptions, ICE has not explained why it cannot simply redact or withhold the material that ICE believes to be exempt, just as it frequently does in the context of its other public productions. And to the extent that ICE suggests—but does not squarely argue—that making redaction decisions would be unduly burdensome because it would require “analyzing each datapoint at the outset,” Dkt. 40-1 at 32, ICE does not explain why any claimed burden could not be alleviated by phased production, starting with tables like the “CSE” table that are of central importance to Plaintiffs’ request. The “CSE” table contains only 32 fields, Long Decl. ¶ 16 & Exh. M, and none of those fields appear to be subject to the statutes that ICE cites in

support of its Exemption 3 argument. Even if other tables may pose thornier problems, ICE has neither identified those problems with specificity nor stated why the risk of potentially difficult redaction decisions in the future relieves it of its duty to start producing nonexempt records now.

## **II. Plaintiffs are entitled to partial summary judgment.**

Even taking ICE’s summary judgment evidence at face value and overlooking the material factual disputes regarding that evidence, Plaintiffs are entitled to partial summary judgment on the present record. ICE does not dispute that Plaintiffs sought records under FOIA and that ICE has withheld them. It is therefore ICE’s burden to justify withholding the records sought, *Seife*, 43 F.4th at 235, and to demonstrate that no reasonably segregable nonexempt records have been withheld, *ACLU Immigrants’ Rights Project*, 58 F.4th at 654. ICE’s evidence is insufficient to carry ICE’s burden with respect to some of the records that Plaintiffs seek.

As explained above, *supra* Part I.A.1, ICE’s disputed evidence that it would be burdensome to produce a single master table that incorporates all of the data that Plaintiffs seek does not contradict the unrebutted evidence that ICE could feasibly make exact copies of the EID tables that form the subject of Plaintiffs’ operative FOIA request and produce those tables, a few at a time, on a rolling basis. For example, ICE could begin producing records that are responsive to Part (1) of Plaintiffs’ request by providing a copy of the “CSE” table. It could then begin producing copies of the tables that are directly linked to the “CSE” table, followed by copies of the tables that are indirectly linked to the “CSE” table. ICE has produced no evidence to suggest that such a course of action would be unfeasible, and it therefore cannot carry its burden to defeat Plaintiffs’ FOIA claim, at least in part, even if all factual disputes are resolved in ICE’s favor.

Similarly, Plaintiffs’ evidence shows that at least some of the tables and fields Plaintiffs seek are not even arguably subject to a FOIA exemption. Again, the “CSE” table is a critical

example. It contains 32 fields, none of which appear to contain SPI and any one of which could be redacted in straightforward fashion if ICE contended that it did, in fact, implicate one of ICE's claimed concerns. *See Long Decl.* ¶ 16 & Exh. M. ICE's evidence presents no reason why the "CSE" table, at minimum, could not be produced without further delay.

Now well over a year since Plaintiffs submitted their FOIA request, ICE has not produced a single record in response. Plaintiffs accept that disputes may arise over particular records and that ICE may well present valid justifications for withholding or redacting certain portions of the requested records. But to prevail on Plaintiffs' FOIA claim, ICE must show that *no* responsive records can appropriately be produced. Even the current, pre-discovery record establishes beyond genuine dispute that ICE cannot hope to do so.

**III. In the alternative, a ruling on summary judgment should be deferred pending discovery.**

Alternatively, should this Court hold that fact disputes foreclose a grant of partial summary judgment in Plaintiffs' favor at this time, the Court should defer resolution of the parties' cross-motions until Plaintiffs have had an opportunity to conduct discovery into ICE's claimed defenses. Plaintiffs served a set of discovery demands on ICE on October 31, 2024, at the authorization of Magistrate Judge Dancks, and ICE has not yet responded. *See Sansone Decl.* ¶¶ 22, 26. Under Federal Rule of Civil Procedure 56(d), this Court has discretion to defer ruling on summary judgment until the discovery process is complete, and there are strong reasons to exercise that discretion in Plaintiffs' favor here.

First, ICE's motion rests on factual representations that appear inconsistent with ICE's previous representations and practices. For example, Mr. Gibney and Ms. Lynch make claims about the size of the EID's dataset that are inconsistent with documents ICE has produced in the context of a separate litigation. *See supra* pp. 9, 20. Mr. Gibney's claims about whether the EID

is structured to produce person-by-person data are inconsistent with numerous past representations that ICE has made, and with its consistent practice of releasing case-by-case information to the public. *See supra* pp. 9–10, 21–22. Ms. Lynch and Mr. Fontaine invoke privacy and cybersecurity concerns that are belied by the nature and contents of the public productions of EID data that ICE has made and continues to make. *See supra* pp. 21–22. And the list could go on. In these circumstances, summary judgment should either be denied, or a ruling should await discovery. *See Carney*, 19 F.3d at 812 (explaining that a “showing of bad faith” or “tangible evidence” contradicting an agency’s account can “justify discovery” in a FOIA case).

Second, the discovery served by Plaintiffs goes directly to factual disputes at the heart of ICE’s summary judgment arguments. Among other things, Plaintiffs seek information about the feasibility of simply producing a copy of the “CSE” table and transmitting it to Plaintiffs, the number of tables that are directly or indirectly linked to the “CSE” table and the feasibility of copying and producing those tables, the amount and segregability of SPI contained in the EID, and past instances in which ICE has produced the sort of metadata described in Mr. Fontaine’s declaration without incident. This discovery is clearly “relevant to [the parties’] claim[s] or defense[s] and proportional to the needs of the case,” and it is particularly appropriate given ICE’s “access to relevant information.” Fed. R. Civ. P. 26(b)(1).

Third, Plaintiffs have been diligent in pursuing discovery. *See Elliott*, 84 F.4th at 493 (listing a party’s “effort … to obtain” discovery as a factor in the Rule 56(d) analysis (quoting *Lunts v. Rochester City Sch. Dist.*, 515 F. App’x 11, 13 (2d Cir. 2013) (summary order))). At the time Plaintiffs filed suit, they had requested records under FOIA, and ICE had neither produced the records nor offered an explanation as to why it would not do so. *See* Sansone Decl. ¶ 4. In that posture, Plaintiffs agreed with ICE that targeted discovery demands could not be crafted

until after ICE had come forward with a justification for withholding the records, *id.* ¶ 6, but Plaintiffs informed both ICE and the Court that they believed discovery would likely be necessary once ICE had come forward with its asserted justifications, *id.* ¶ 11; *see* Dkt. 35 at 2. ICE came forward with its asserted justifications for the first time when it filed its motion for summary judgment on October 1, 2024. *See* Sansone Decl. ¶ 13. Counsel for Plaintiffs met and conferred with counsel for ICE within a week afterwards, and Plaintiffs put the issue of discovery before the Court just two days after that. *Id.* ¶ 21; *see* Dkt. 43.

Finally, allowing the discovery process to conclude before ruling on ICE’s motion will conserve resources for the Court and for the parties. Denying ICE’s motion before Plaintiffs have had the opportunity to build a complete evidentiary record around the key factual disputes could allow ICE to file a second motion, supported by new declarations that will create further disputes and that will require the parties to author (and the Court to analyze) further rounds of briefing. Courts regularly bemoan this inefficient practice and the resulting delays that too often encumber FOIA litigation. *See, e.g., Akel v. DOJ*, No. 20-cv-03240, 2024 WL 939974, at \*2 (D.D.C. Mar. 4, 2024) (“The type of iterative process represented by this case—and all too many FOIA cases—constitutes a burden on the time [and] resources of all involved, and, more importantly, it is at odds with the statutory design, which attempts to foster expedition.”); *Families for Freedom v. CBP*, 837 F. Supp. 2d 331, 337 (S.D.N.Y. 2011) (“After nearly two years of inadequate searches, six sworn declarations, numerous letters and briefs and in-person conferences, the Court’s patience has worn out.”). This Court should not invite such inefficiency here.

## CONCLUSION

This Court should deny ICE’s motion for summary judgment, grant partial summary judgment in favor of Plaintiffs, and order ICE to begin producing nonexempt records, such as the

“CSE” table, that ICE can deliver without implicating its disputed burdensomeness concerns. In the alternative, this Court should defer ruling on ICE’s motion until Plaintiffs have had the opportunity to conduct discovery and to supplement the record as appropriate.

Dated: November 8, 2024

Respectfully submitted,

/s/ Nicolas A. Sansone

Nicolas A. Sansone (admitted pro hac vice)  
Michael T. Kirkpatrick (admitted pro hac vice)  
Public Citizen Litigation Group  
1600 20th Street NW  
Washington, DC 20009  
(202) 588-7714  
nsansone@citizen.org

*Counsel for Plaintiffs*